UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

LYLE HARTOG, *on behalf of himself and all other similarly situated,*

Plaintiff,

v.

ORTHOPEDICSNY, LLP,

Defendant.

Case No.: 1:24-cv-1368 (LEK/ML)

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Lyle Hartog ("Plaintiff"), on behalf of himself and all others similarly situated ("Class Members") (collectively, the "Class"), files this Class Action Complaint ("Complaint") against Defendant OrthopedicsNY, LLP ("OrthopedicsNY" or "Defendant") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to safeguard and secure the personally identifiable information ("PII") and protected health information ("PHI", and together with the PII, the "Private Information") of its former, present, prospective patients, their family members, and other individuals associated, including Plaintiff, around the nation. At Defendant's request, Plaintiff provided his PII and PHI to Defendant, which maintained Plaintiff's and Class Members' PII and PHI but failed to sufficiently secure them.

2. As a result of Defendant's negligence, cybercriminals were able to gain access to Defendant's corporate systems, which contain data records and sensitive and valuable PII and PHI ("Data Breach").

3. On or around December 28, 2023, Defendant became aware of suspicious activity on its network and discovered that an unauthorized third party has accessed certain systems.

4. Defendant notified affected individuals, including Plaintiff, of the breach in a letter dated October 30, 2024 (the "Notice Letter"), attached hereto as Exhibit 1.

5. In the Notice Letter, Defendant confirmed that files containing Plaintiff's and Class Members' Private Information, including first and last name, mailing address, date of birth, social security number, driver's license number, passport number, financial account information, health insurance information, and/or protected health information. , had been accessed or copied during Data Breach.[1]

6. OrthoNY is a 70-provider orthopedic group serving upstate New York, including the Albany, Schenectady, and Saratoga regions.[2] Since its establishment in 2014, OrthoNY has expanded through strategic mergers and acquisitions.[3] It handles over 177,000 patient visits annually and performs approximately 25,000 surgeries each year.[4]

7. Upon information and belief, the total number of individuals whose PII and PHI was exposed due to Data Breach is estimated to be substantial, including current, former, and prospective patients and individuals associated with them.

---

[1] *See* Exhibit 1.

[2] *OrthoNY's 70-provider Orthopedic Group Streamlined Patient Billing to Generate $860,000 in Additional Revenue with Millennia*, MILLENNIA**,** https://millenniapay.com/success-story/ortho-ny/#:~:text=With%20MRI%20and%20x%2Dray,and%2025%2C000%20surgeries%20per%20year (last visited Nov. 8, 2024).

[3] *Id.*

[4] *Id.*

8. Armed with the PII and PHI accessed in Data Breach, data thieves can commit a variety of crimes, including opening new financial information in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health insurance information to submit claims with their insurance provider, using Class Members' health information to get prescription drugs, and using Class Members' PII and PHI to target other phishing and hacking intrusions.

9. Plaintiff has significant concerns about the security of his personal data. Since the breach, Plaintiff received fraudulent alerts notifying him that his information was exposed on the dark web.

10. Defendant owed a non-delegable duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard its PII and PHI against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect PII and PHI of its current, former, and prospective patients and individuals associated with them from unauthorized access and disclosure.

11. As a result of Defendant's inadequate security and breach of its duties and obligations, Data Breach occurred, and Plaintiff's and Class Members' PII and PHI was accessed and disclosed. This action seeks to remedy these failings and the harm caused to Plaintiff and Class Members as a result. Plaintiff brings this action on behalf of himself and all persons whose PII and PHI was exposed because of Data Breach.

12. As a result of Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of financial fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant's data security system, future annual audits, and fully adequate identity monitoring services funded by Defendant.

14. Plaintiff, on behalf of himself and other Class Members, asserts claims for negligence and negligence *per se*, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, equitable relief, and other relief authorized by law.

PARTIES

15. On or around December 28, 2023, Defendant became aware of suspicious activity on its network and discovered that an unauthorized third party had accessed certain systems. Upon investigation, Defendant confirmed that files containing Plaintiff's and Class Members' PII and PHI, including first and last name, mailing address, date of birth, social security number, driver's license number, passport number, financial account information, health insurance information, and/or protected health information, had been accessed or copied.

16. Plaintiff is a resident of Saratoga County, New York. As a current patient at Defendant's facility, Plaintiff provided his PII and PHI to Defendant upon Defendant's request. Plaintiff received a letter from Defendant, dated October 30, 2024, notifying him that his Private Information was impacted in Data Breach.

17. Defendant is a New York limited liability partnership that maintains its principal place of business located at 121 Everett Road, Albany, New York 12205.

18. Had Plaintiff known that Defendant would not adequately protect his and Class Members' PII, he would not have provided his PII and PHI to Defendant or any of its affiliates.

19. At all relevant times, Plaintiff is and continues to be a member of the Class.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) because (i) there are 100 or more Class Members, (ii) at least one Class Member is a citizen of a state that is diverse from Defendant's citizenship, and (iii) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

21. This Court has general personal jurisdiction over Defendant because Defendant is a citizen of New York. Moreover, Defendant has sufficient minimum contacts in New York, and Defendant engaged in the conduct underlying this action in New York, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class Members' PII and PHI. Defendant intentionally availed themselves of this jurisdiction by marketing and selling products and services and accepting and processing payments for those products and services within New York.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because substantial portion of the acts and transactions that constitute the violations of law complained of herein occurred in Saratoga County, New York, and Defendant conducts substantial business across Albany, Clifton Park, Schenectady, and Saratoga—all of which are within this Judicial District

FACTUAL ALLEGATIONS

Overview of Defendant

23. Defendant OrthoNY is a 70-provider orthopedic group serving upstate New York, including the Albany, Schenectady, and Saratoga regions. Since its establishment in 2014, OrthoNY has expanded through strategic mergers and acquisitions. It handles over 177,000 patient visits annually and performs approximately 25,000 surgeries each year. Upon information and belief, the number of patient visits is expected to have gradually increased.

24. Plaintiff was required to provide his Private Information, as a condition to receive medical treatment from Defendant.

25. To proceed with the medical services that Defendant handles, Defendant's patients and associated individuals, such as Plaintiff and Class Members, are required to, and did, provide Defendant directly with sensitive PII and PHI.

26. In the regular course of its business, Defendant collects, stores, and maintains the PII and PHI it receives from current, former, and prospective patients and individuals associated with them.

27. By creating and maintaining massive repositories of PII and PHI, Defendant has provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

Data Breach and Notice Letter

28. On or around December 28, 2023, Defendant became aware of the Data Breach, and that it was a target of a ransom attack.

29. After 252 days, Defendant, on September 5, 2024, was finally able to conclude its internal investigation on the Data Breach.[5] Defendant again waited until October 30, 2024, 50 days after the conclusion of the investigation, to notify Data Breach victims.[6]

30. In or around August 2024, Plaintiff received an electronic notification from his credit card provider that his information was exposed on the dark web and was instructed to put a fraud alert on all three major credit reporting agencies.

[5] *Id.*

[6] *Id.*

31. In November 2024, Plaintiff received a letter from Defendant, dated October 30, 2024, notifying him that his Private Information was impacted in Data Breach.

32. While Defendant claims in its Notice Letter that it takes "the security of [its patients'] personal information seriously," Defendant failed to do so. Specifically, while Defendant offers complimentary identity protection services, it places the burden on Data Breach victims to reach out to the service provider to resolve fraudulent activities with limited instructions, and a tight deadline to enroll within 90 days from the date of the notice letter.[7]

33. To date, Defendant has not disclosed crucial information, including, but not limited to, the identity of the hacking group responsible for Data Breach, how the cybercriminals were able to exploit vulnerabilities in Defendant's IT security systems, or any steps taken by Defendant to safeguard its systems meeting the standard of specificity expected from Data Breach victims.

34. Upon information and belief, Defendant's inadequate cybersecurity measures, failure to properly train employees, and failure to monitor systems allowed Data Breach to occur.

35. Defendant failed to detect and stop Data Breach in a timely manner and delayed notifying affected individuals about the incident. Although Defendant became aware of Data Breach on or around December 28, 2023, Defendant did not begin posting notifications about Data Breach to its website until November 4, 2024, and did not directly notify Plaintiff of Data Breach until October 30, 2024.

36. As a result of Data Breach, Plaintiff's and Class Members' PII and PHI are exposed to unauthorized individuals, placing them at risk of identity theft and other financial harm.

37. As a result of Data Breach, Plaintiff and Class Members suffered ascertainable losses from the loss of the value in their private and confidential information, loss of the benefit

[7] *See* Exhibit 1.

of their contractual bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

38. Plaintiff and Class Members have and will continue to incur out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

39. Defendant's actions, including the delayed notification of Data Breach and the significant lag in investigation, caused additional harm to Plaintiff and Class Members by limiting their ability to take immediate steps to protect themselves from identity theft.

40. Defendant did not use reasonable security procedures to safeguard the sensitive information of Plaintiff and Class Members.

41. Defendant's systems hacked by cybercriminals contained Plaintiff's and Class Members' PII and PHI that was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

42. Plaintiff and Class Members provided their PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligation to keep such information confidential and secure from unauthorized access.

43. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from unauthorized disclosure.

Defendant Knew That Criminals Target PII and PHI

44. In its regular course of business, Defendant accumulates highly private PII and PHI of its current, former, and prospective clients and individuals associated with matters, directly or indirectly, including families of current, former, and prospective clients.

45. In collecting and maintaining its PII and PHI, Defendant owed a non-delegable duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized access and disclosure.

46. Cyber-attacks against healthcare organizations, such as Defendant, are targeted. According to the 2023 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[r]ansomware attacks are often state-sponsored and highly organized and sophisticated. Since as early as 2018, healthcare organizations have been concerned about ransomware attacks. 2023 was no exception, as the number of ransomware leak sites divulging sensitive information, such as patient information, have greatly increased."[8] Hospitals have "emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[9]

[8] *2023 HIMSS Healthcare Cybersecurity Survey*, HIMSS 13, https://gkc.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf (last visited Nov. 8, 2024).

[9] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXEC., https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (Apr. 4, 2019).

47. Defendant had obligations created by Health Insurance Portability and Accountability Act ("HIPAA"), contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

48. As a medical institution, Defendant understood the need to protect the PII and PHI it collects and maintains, and to prioritize its data security. In particular, Defendant was fully aware of and understood the need to protect the PII and PHI of its patients and associated individuals.[10]

49. Despite its acknowledged duty, Defendant failed to implement adequate cybersecurity safeguards and policies to protect personal information of current, former, and prospective patients and individuals associated with their matters, including Plaintiff. Defendant did not properly train its IT or data security staff to prevent, detect, or stop breaches, leaving its systems vulnerable to exploitation by cybercriminals.

50. PII and PHI is of great value to hackers and cybercriminals, and the data comprised in Data Breach can be used in variety of unlawful manners.

51. PII and PHI can be used to distinguish, identify, or trace an individual's identity, such as name, Social Security number, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as birthdate, birthplace, and mother's maiden name.

52. Given the nature of this breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

[10] *Privacy*, ORTHONY, https://www.orthony.com/privacy/ (last visited Nov. 8, 2024) ("We may also track where you go or what you read in our Website so that we can provide you with effective follow up information, but only if you have given us explicit permission to do so by filling out a form that asks you if we may do so.").

53. Indeed, the cybercriminals who possess Class Members' PII and PHI can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

54. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' PII.[11]

55. As a result of the notoriety of cyberattacks on systems like Defendant's, several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack, like Data Breach.

56. In light of the high-profile data breaches in similar industries and large businesses, and a wealth of relevant guidance and news reports at Defendant' disposal, Defendant knew or should have known that cybercriminals would target its electronic records and PII of current, former, and prospective clients and individuals associated with their matters.

57. These data breaches have been a consistent problem for the past several years, providing Defendant sufficient time and notice to improve the security of its systems and engage in stronger, more comprehensive cybersecurity practices.

[11] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Sept. 30, 2024).

58. PII/PHI is a valuable property right.[12] The value of PII/PHI as a commodity is measurable.[13] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[14] American companies are estimated to have spent over $19 billion acquiring consumers' personal data in 2018.[15] In fact, PII/PHI are so valuable to identity thieves that once disclosed, criminals often trade it on the cyber black-market, or the dark web, for many years.

59. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, and other PII/PHI directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

60. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy — and the amount is considerable. Indeed,

---

[12] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[13] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[14] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[15] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[16]

61. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

62. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

63. Accordingly, Defendant clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the PII and PHI stored in its unprotected files and the massive amount of PII and PHI it maintains.

64. Equally, at all relevant times, Defendant knew or should have known that Plaintiff's and all other Class Members' PII and PHI were targets for malicious actors.

Theft of PII and PHI has Grave and Lasting Consequences for Victims

65. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of their financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[17]

---

[16] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[17] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

66. Plaintiff and Class Members who have fallen victim to a data breach suffer real harms.[18]

67. Data breaches represent a significant problem for victims who have already experienced the inconvenience and disruption associated with a cyber-attack.

68. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[19] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[20]

69. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact on their credit.

70. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security numbers to open financial accounts, receive government benefits, and incur charges and credit in

---

[18] Ying Hu, *Mainstreaming Unjust Enrichment and Restitution in Data Security Law*, 13 U.C. IRVINE L. REV. 855, 872 (2023) ("Plaintiff who have fallen victim to a data breach suffer real harms. There is a higher chance that their personal data will be used against their interests: wrongdoers might use that data to locate and injure them….").

[19] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[20] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Sept. 30, 2024).

a person's name.[21] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim's credit rating.

71. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[22]

72. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that Private Information has considerable market value.

73. Theft of PHI is particularly problematic because: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[23]

74. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims

---

[21] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[22] *Id.* at 2, 9.

[23] *See Medical Identity Theft*, Federal Trade Commission Consumer Information http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Oct. 4, 2024).

themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

75. There may be a time lag between when PII is stolen and when it is used.[24] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade it on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, Social Security numbers, and other PII directly on various internet websites, making the information publicly available.

76. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who companies employ to find flaws in their computer systems, stating, "If I have your

[24] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

[25] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 34 (emphasis added).

name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[26]

77. Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 and up.[27]

78. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

79. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[28]

80. Plaintiff and Class Members must vigilantly monitor their financial accounts and their family members' accounts for many years to come.

81. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market. Plaintiff and all other Class Members have suffered injury and damages, including, but not limited to (i) a substantially increased risk of

---

[26] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[27] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed December 10, 2020).

[28] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://efraudprevention.com/pub/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Oct. 4, 2024).

identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; and (v) lost time and money incurred to mitigate and remediate the effects of Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

Damages Sustained by Plaintiff and the Other Class Members

82. Plaintiff is very careful about sharing his sensitive PII/PHI. Plaintiff has never knowingly transmitted unencrypted PII/PHI over the internet or any other unsecured source.

83. Because of Data Breach, Defendant directed Plaintiff to take certain steps to protect his PII and otherwise mitigate his damages.

84. Because of Data Breach, Plaintiff spent time dealing with the consequences of Data Breach, which includes time spent self-monitoring financial accounts, signing up for credit protection services and setting up credit alerts, freezing credit reports, and changing passwords for his accounts. This time has been lost forever and cannot be recaptured. And this time was spent at Defendant's direction by way of Data Breach notice where Defendant recommended that Plaintiff mitigate her damages by, among other things, monitoring his accounts for fraudulent activity.

85. Since Data Breach, Plaintiff has been notified that his Private Information was exposed on the dark web. Plaintiff suffered emotionally over the stress resulting from Data Breach and his substantially increased risk of identity theft, such as the possibility of criminals using his PII/PHI to open bank accounts or commit other frauds.

86. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII/PHI that Plaintiff entrusted to Defendant, which was compromised because of Data Breach. Plaintiff suffered lost time, annoyance, interference, insecurity, and inconvenience because of Data Breach and has increased concerns for the loss of his privacy.

87. Plaintiff and other Class Members have suffered injury and damages, including but not limited to Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of their financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[29]

88. As a result, Plaintiff and all other Class Members have suffered injury and damages, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; and (v) lost time and money incurred to mitigate and remediate the effects of Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

[29] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

89. Furthermore, Defendant has failed to provide adequate compensation to Plaintiff and Class Members harmed by its negligence. To date, Defendant has offered Plaintiff and Class Members a complimentary credit monitoring service that is available for a limited time period of 12 months from the date of enrollment. More devastating is that this complimentary monitoring service will be rendered unusable unless Plaintiff and Class Members enroll within 90 days from the date each Notice Letter was sent to them. Even if affected individuals accept the credit monitoring service, it will not provide them with any compensation for the costs and burdens associated with fraudulent activity resulting from Data Breach that took place prior to signing up for the service. Defendant has not offered Class Members any assistance in dealing with the IRS or state tax agencies. Nor has Defendant offered to reimburse Plaintiff and Class Members for any costs incurred as a result of falsely filed tax returns, a common consequence of data breaches.

90. The offered credit monitoring service is inadequate to protect Class Members from the threats they face. It does nothing to protect against identity theft. Instead, it only provides various measures to identify identity theft once it has already been committed.

91. The offered credit monitoring services are also wholly inadequate in that they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI.

92. Yet, Defendant has failed to provide transparency regarding the cause of Data Breach, instead placing the burden on Plaintiff and Class Members to address the issue themselves.

CLASS ACTION ALLEGATIONS

93. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

94. Plaintiff proposes the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> **All individuals whose PII and PHI was accessed by unauthorized persons as a result of Data Breach.**

95. Plaintiff reserves the right to amend the above definition or to propose other or additional classes in subsequent pleadings and/or motions for class certification.

96. Plaintiff is a member of the Class.

97. Excluded from the Class are Defendant, its affiliates, parents, subsidiaries, officers, agents, directors, the judge(s) presiding over this matter, and the clerks of said judge(s).

98. This action seeks both injunctive relief and damages.

99. Plaintiff and the Class satisfy the requirements for class certification for the following reasons set forth below.

100. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. While the exact number of Class Members is unknown at this time, Class Members are readily identifiable in Defendant's records, which will be a subject of discovery. Upon information and belief, there are more than 177,000 Class Members in the Class as of November 8, 2024,[30] and the number is expected to continue growing.

[30] *See supra* ¶ 6.

101. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;
b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in Data Breach;
c. Whether Defendant's data security systems prior to and during Data Breach complied with applicable data security laws and regulations;
d. Whether Defendant's data security systems prior to and during Data Breach were consistent with industry standards;
e. Whether Defendant owed a duty to Class Members to safeguard their PII and PHI;
f. Whether Defendant breached its duty to Class Members to safeguard their PII and PHI;
g. Whether criminals obtained Class Members' PII and PHI in Data Breach;
h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
j. Whether Defendant owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendant breached that duty;
k. Whether Defendant's conduct was negligent;
l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
m. Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

102. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and violations of law. Plaintiff and Class Members all had their PII and PHI stolen in Data Breach. Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

103. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. His interests do not conflict with the interests of the Class.

104. Plaintiff and his chosen attorney – Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG" or "Plaintiff's Counsel") – are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint. In particular, FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. Plaintiff's Counsel is competent in the relevant areas of the law and has sufficient experience to vigorously represent Plaintiff and Class Members. Finally, Plaintiff's Counsel possesses the financial resources necessary to ensure that a lack of financial capacity will not hamper the litigation and is willing to absorb the costs of the litigation.

105. **Predominance.** The common issues identified above arising from Defendant's conduct predominate over any issues affecting only individual Class Members. The common issues hinges on Defendant's common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

106. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large number of injured persons, to keep the courts from becoming paralyzed by hundreds—if not thousands—of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation possible.

107. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which, in any event, might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of monetary damages due and terms of equitable relief, can be determined in this single proceeding rather than in multiple individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief to Class Members and Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only current, former, and prospective patients of Defendant and individuals associated with their matters, directly or indirectly, the legal and factual issues are narrow and easily defined, and Class Membership is limited. The Class does not contain so many persons that would make thecClass notice procedures unworkable or overly expensive. The identity of Class Members can be identified from Defendant's records, such that direct notice to Class Members would be appropriate.

108. **Injunctive Relief.** Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTIONS

COUNT 1
NEGLIGENCE

(ON BEHALF OF PLAINTIFF AND CLASS MEMBERS)

109. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

110. As requested by Defendant in relation to its legal proceedings, Plaintiff and Class Members provided Defendant with their PII and PHI.

111. By collecting and storing their PII and PHI, at all times relevant, Defendant owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in their possession, custody, or control.

112. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with statutory and industry standards and to ensure that its systems and networks and the personnel responsible for them adequately protected PII and PHI.

113. Defendant knew the risks of collecting and storing Plaintiff's and all other Class Members' PII and PHI and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted companies that store PII and PHI in recent years.

114. Given the nature of Defendant's business, the sensitivity and value of PII and PHI Defendant maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities in its systems and prevented Data Breach from occurring.

115. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as the common law.

Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

116. Defendant's duty to use reasonable security measures under HIPAA required Defendant to reasonably protect confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1), (2).

117. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA. 45 C.F.R. § 164.530(b)(1)

118. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

119. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

120. According to the University of Illinois Chicago (UIC), "protecting health information (PHI) from cyberattacks is vital."[31]

121. UIC has identified several strategies and best practices that, at a minimum, should be implemented by healthcare providers like Defendant, including but not limited to: "[e]ncrypting data ensures that even if data is breeched, it cannot be read without the decryption key," "[i]mplementing strict access controls helps ensure that only authorized personnel can access

[31] *Healthcare Cybersecurity: Health Informatics Safeguards Patient Data*, UNIV. OF ILL. CHIC., https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/ (last visited Nov. 8, 2024).

sensitive information," "[c]ontinuous monitoring and regular audits can help detect unusual activities and potential breaches early," and "[e]ducating employees about best practices and how to recognize phishing attempts can reduce the risk of human error."[32]

122. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security (CIS) released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these guidelines.[33]

123. Other cybersecurity best practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and the protection of physical security systems; protecting against any possible communication system; and training staff regarding critical points.

124. Upon information and belief, Defendant failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness.

125. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI by failing to design,

---

[32] *Id.*

[33] *CIS Benchmarks™ FAQ*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Nov. 8, 2024).

adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it, including Plaintiff's and Class Members' PII and PHI.

126. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of current, former, and prospective patients and individuals associated with their matters that Defendant were aware, or should have been aware, could be injured by inadequate data security measures.

127. Plaintiff and Class Members have no ability to protect their PII and PHI that was or remains in Defendant's possession.

128. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII and PHI to unauthorized individuals.

129. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

130. Defendant's conduct was negligent and departed from reasonable standards of care, including but not limited to failing to adequately protect Plaintiff's and Class Members' PII and PHI and failing to provide them with timely notice that their Private Information had been compromised.

131. Neither Plaintiff nor Class Members contributed to Data Breach and subsequent misuse of their PII and PHI, as described in this Complaint.

132. By failing to provide timely and complete notification of Data Breach to Plaintiff and Class Members, Defendant prevented them from proactively taking steps to secure their PII and PHI and mitigate the associated threats.

133. As a result of Defendant's above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused Data Breach, Plaintiff and all other Class Members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; and (vi) lost time and money incurred to mitigate and remediate the effects of Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II
NEGLIGENCE *PER SE*

(ON BEHALF OF PLAINTIFF AND CLASS MEMBERS)

134. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

135. Defendant had duties by statute to ensure that all information it collected and stored was secure and that it maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and Class Members' PII and PHI.

136. Defendant' duties arise from, *inter alia*, Section 5 of the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45(a)(1) ("FTCA"), which prohibits "unfair . . . practices in or affecting

commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

137. The FTC has published numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the personal customer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[34]

138. Furthermore, businesses maintaining health information must ensure "health data practices ae not substantially injuring consumers, including by invading their privacy." [35] In fact, FTC is taking high priority in protecting consumers' protected health information spanning treatments, diagnoses to any health information that enables an inference about consumer's health.[36]

139. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[34] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[35] *Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach (last visited Nov. 8, 2024).

[36] *See id.*

unfair act or practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses such as Defendant must take to meet their data security obligations and effectively put Defendant on notice of these standards.

140. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all Class Members' PII and PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI, including, specifically, the substantial damages that would result to Plaintiff and other Class Members.

141. Defendant's violation of the FTCA constitutes negligence *per se*.

142. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

143. The harm occurring as a result of Data Breach is the type of harm against which Section 5 of the FTCA was intended to guard.

144. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

145. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violation of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual

harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; and (vi) lost time and money incurred to mitigate and remediate the effects of Data Breach, including the increased risks of identity theft they face and will continue to face. Defendant's violation of the FTCA constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from Data Breach.

146. Defendant owed a duty of care to Plaintiff and other Class Members because they were foreseeable and probable victims of any inadequate security practices.

147. It was foreseeable that Defendant's failure to use reasonable measures to protect PII/PHI and provide timely notice of Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and other Class Members were reasonably foreseeable.

148. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and other Class Members: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring

and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF IMPLIED CONTRACT

(ON BEHALF OF PLAINTIFF AND CLASS MEMBERS)

149. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

150. When Plaintiff and Class Members provided their PII and PHI to Defendant directly or indirectly as a pre-condition to receive medical treatment, they entered into implied contracts with Defendant.

151. Pursuant to these implied contracts, in exchange for the consideration and PII and PHI provided by Plaintiff and Class Members, Defendant agreed to, among other things, and Plaintiff understood that Defendant would: (1) provide medical treatment to Plaintiff and Class Members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII and PHI; and (3) protect Plaintiff's and Class Members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

152. The protection of PII and PHI was a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and Defendant, on the other.

153. Plaintiff and Class Members performed their obligations under the implied contract when they provided Defendant with their PII and paid for the services from Defendant.

154. Plaintiff and Class Members would not have entrusted their PII and PHI to Defendant in the absence of such an implied contract.

155. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards. Had Plaintiff and Class Members known that Defendant would not adequately protect its employees' and former employees' PII and PHI, they would not have agreed to employment by Defendant.

156. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of Data Breach.

157. Specifically, Defendant did not maintain the privacy of Plaintiff' and Class Members' Private Information, as evidenced by its late notification of Data Breach to Plaintiff and Class Members. Furthermore, Defendant did not comply with industry standards, the standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and Class Members' Private Information, as set forth above.

158. Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

159. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received healthcare and other services that were of a diminished value compared to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

160. As a direct and proximate result of Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including

without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

161. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of Data Breach.

162. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
BREACH OF FIDUCIARY DUTY

(ON BEHALF OF PLAINTIFF AND CLASS MEMBERS)

163. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

164. In providing their Private Information to Defendant, Plaintiff and Class Members justifiably placed special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class Members to safeguard and keep confidential that Private Information.

165. Defendant accepted the special confidence placed in it by Plaintiff and Class Members. There was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of their Private Information.

166. In light of the special relationship between Defendant, Plaintiff, and Class Members, whereby Defendant became the guardian of Plaintiff's and Class Members' Private Information, Defendant accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and Class Members. This duty included safeguarding Plaintiff's and Class Members' Private Information.

167. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its medical relationship with its patients, in particular, to keep secure Private Information of those patients.

168. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, or give notice of Data Breach in a reasonable and practicable period of time.

169. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of its computer systems containing Plaintiff's and Class Members' Private Information.

170. Defendant breached the fiduciary duties it owed to Plaintiff and Class Members by failing to timely notify and/or warn them of Data Breach.

171. Defendant breached its fiduciary duties by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

172. Defendant breached its fiduciary duties by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1).

173. Defendant breached its fiduciary duties by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

174. Defendant breached its fiduciary duties by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii).

175. Defendant breached its fiduciary duties by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2).

176. Defendant breached its fiduciary duties by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3).

177. Defendant breached its fiduciary duties by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(94).

178. Defendant breached its fiduciary duties by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502, *et seq*.

179. Defendant breached its fiduciary duties by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

180. Defendant breached its fiduciary duties by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. § 164.530(c).

181. Defendant breached its fiduciary duties by otherwise failing to safeguard Plaintiff' and Class Members' Private Information.

182. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

183. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT

(ON BEHALF OF PLAINTIFF AND CLASS MEMBERS)

184. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

185. This claim is pleaded in the alternative to the foregoing causes of actions.

186. Defendant, by way of its acts and omissions, knowingly and deliberatively enriched themselves by saving the costs they reasonably should have expended on security measures to secure Plaintiff's and Class Members' PII and PHI.

187. Instead of providing for a reasonable level of security that would have prevented Data Breach—as is common practice among companies entrusted with such PII and PHI—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class Members.

188. Nevertheless, Defendant continued to obtain the benefits conferred on them by Plaintiff and Class Members.

189. Plaintiff and Class Members, on the other hand, suffered harm as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resultant Data Breach disclosing Plaintiff's and Class Members' PII and PHI, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of, *inter alia*, attempted identity theft, time and expenses mitigating harms, diminished value of Private Information, loss of privacy, and increased risk of harm.

190. Thus, Defendant engaged in opportunistic conduct in spite of their duties to Plaintiff and Class Members, wherein it profited from interference with Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to

permit Defendant to retain the benefits it derived as a consequence of its conduct.

191. Accordingly, Plaintiff, on behalf of himself and Class Members, respectfully request this Court award relief in the form of restitution and/or compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and Class Members;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper, including additional protections for Plaintiff and Class Members.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 12, 2024

Respectfully Submitted,

s/ Todd S. Garber

Todd S. Garber
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com

Attorneys for Plaintiff and the Proposed Class